EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Robert C. Kowert Registration No. 39,255 on January 26, 2012.

The application has been amended as follows:

Claims **1** and **21** have been amended as follows:

1. (Currently Amended) A method implemented in a device supporting a public-key cryptography application, the method comprising:

feeding back, using a first arithmetic circuit comprising a first plurality of arithmetic structures, ~~feeding back~~ high order bits of a previously executed single arithmetic instruction of a processor instruction set in the public-key cryptography application, generated by the first arithmetic circuit, to a second arithmetic circuit comprising a second plurality of arithmetic structures;

generating, using the second arithmetic circuit, ~~generating~~ a first partial result of a currently executing single arithmetic instruction of the processor instruction set in the public-key cryptography application, wherein the currently executing single arithmetic instruction does not include an explicit source operand for specifying the high order bits, the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number, the summing of the high order bits being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic circuit;

storing the first partial result; and

using the stored first partial result in a subsequent computation in the public-key cryptography application.

21. (Currently Amended) A method implemented in a device supporting a public-key cryptography application, the method comprising:

feeding back, using a first arithmetic circuit comprising a first plurality of arithmetic structures, ~~feeding back~~ high order bits of a previously executed single arithmetic instruction of a processor instruction set in the public-key cryptography application, generated by the first arithmetic circuit to a second arithmetic circuit comprising a second plurality of arithmetic structures;

supplying a third number to the second arithmetic circuit;

generating, using the second arithmetic circuit, ~~generating~~ a first partial result of a currently executing single arithmetic instruction of the processor instruction set in the public-key cryptography application, wherein the currently executing single arithmetic instruction does not include an explicit source operand for specifying the high order bits, the first partial result being a representation of the high order bits summed with low order bits of a result of a first number multiplied by a second number and with the third number, the summing being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic circuit;

storing the first partial result; and

using the first partial result in a subsequent computation in the public-key cryptography application.

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance.

Claims **1, 21, 38, 53, 66, 67** are allowed based on the following:

The prior art of record, considered individually or in combination, fails to fairly show or suggest: a first arithmetic circuit comprising a first plurality of arithmetic structures feeding back high order bits of a previously executed single arithmetic instruction of a processor instruction set in the public-key cryptography application, generated by the first arithmetic circuit, to a second arithmetic circuit comprising a second plurality of arithmetic structures; and the second arithmetic circuit generating a

first partial result of a currently executing single arithmetic instruction of the processor instruction set in the public-key cryptography application, wherein the currently executing single arithmetic instruction does not include an explicit source operand for specifying the high order bits, the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number, the summing of the high order bits being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic circuit, in addition to the other limitations in a manner as recited in claims **1 - 67**.

Claims **2 - 20** are allowed due to allowed base claim **1**.

Claims **22 - 37** are allowed due to allowed base claim **21**.

Claims **39 - 52** are allowed due to allowed base claim **38**.

Claims **54 - 65** are allowed due to allowed base claim **53**.

So as indicated by the above statements, Applicant's arguments have been considered persuasive, in light of the set of claims with limitations as well as the enabling portions of the specification. The dependent claims further limit the independent claims and are considered allowable on the same basis as the independent claims as well as for the further limitations set forth.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on

Statement of Reasons for Allowance."

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
January 17, 2012

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436